Random Graphs in Cryptography

Adi Shamir

Abstract

Many questions in cryptography can be phrased as algorithmic problems in the theory of random graphs, and the two areas influenced each other considerably over the last 30 years. In this talk I will describe some of these connections, survey the most interesting results, and show some recently discovered techniques how a cryptanalyst can exploit slight deviations from randomness in order to speed up various attacks.